

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 1 年 7 月 1 8 日
Date of Application:

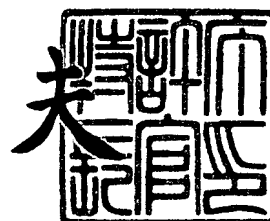
出 願 番 号 特 願 2 0 0 1 - 2 1 7 7 1 0
Application Number:
[ST. 10/C] : [J P 2 0 0 1 - 2 1 7 7 1 0]

出 願 人 エフ・ディー・ケイ株式会社
Applicant(s):

2 0 0 3 年 8 月 7 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



【書類名】 特許願

【整理番号】 IP01401

【あて先】 特許庁長官 殿

【国際特許分類】 H03K 3/84

【発明者】

【住所又は居所】 東京都港区新橋 5 丁目 3 6 番 1 1 号 いわき電子株式会
社内

【氏名】 山本 博康

【発明者】

【住所又は居所】 東京都港区新橋 5 丁目 3 6 番 1 1 号 いわき電子株式会
社内

【氏名】 曾我 竜司

【発明者】

【住所又は居所】 東京都港区新橋 5 丁目 3 6 番 1 1 号 いわき電子株式会
社内

【氏名】 清水 隆邦

【発明者】

【住所又は居所】 東京都港区新橋 5 丁目 3 6 番 1 1 号 いわき電子株式会
社内

【氏名】 鯉淵 美佐子

【特許出願人】

【識別番号】 390022792

【氏名又は名称】 いわき電子株式会社

【代理人】

【識別番号】 100067046

【弁理士】

【氏名又は名称】 尾股 行雄

【電話番号】 03-3543-0036

**【選任した代理人】****【識別番号】** 100096862**【弁理士】****【氏名又は名称】** 清水 千春**【電話番号】** 03-3543-0036**【手数料の表示】****【予納台帳番号】** 008800**【納付金額】** 21,000円**【提出物件の目録】****【物件名】** 明細書 1**【物件名】** 図面 1**【物件名】** 要約書 1**【プルーフの要否】** 要

【書類名】 明細書

【発明の名称】 乱数発生装置

【特許請求の範囲】

【請求項 1】 二つの入力信号の位相差に応じて出力の状態（0 または 1）が確定するフリップ・フロップと、

前記入力信号の位相を調整する位相調整部と、

前記入力信号によるフリップ・フロップ出力の 0 または 1 の出現率が所定の繰り返し周期内で一定値に収束するように前記位相差を制御するフィードバック回路部とで構成される乱数発生装置であって、

前記位相調整部は、それぞれ順を追って作動する位相の粗調整手段および微調整手段を備え、位相調整幅の拡大と位相調整時間の短縮を図ったことを特徴とする乱数発生装置。

【請求項 2】 前記粗調整手段および微調整手段は、前記入力信号を数段階に遅延し出力する遅延回路と、セレクト入力に応じて遅延出力の何れかを選択する選択回路と、前記位相差に応じて前記セレクト入力を制御する可逆カウンタとで、それぞれ構成されることを特徴とする請求項 1 に記載の乱数発生装置。

【請求項 3】 二つの入力信号の位相差に応じて出力の状態（0 または 1）が確定するフリップ・フロップと、

前記入力信号の位相を調整する位相調整部と、

前記入力信号によるフリップ・フロップ出力の 0 または 1 の出現率が所定の繰り返し周期内で一定値に収束するように前記位相差を制御するフィードバック回路部とで構成される乱数発生装置であって、

前記位相調整部は、前記入力信号を数段階に遅延し出力する遅延回路と、セレクト入力に応じて遅延出力の何れかを選択する選択回路と、前記位相差に応じて前記セレクト入力を制御する可逆カウンタとで構成されており、

且つ、0 または 1 の出現率の正規分布と前記繰り返し周期内における 0 または 1 の出現回数を対比し、当該出現回数に対応する前記正規分布の位置に応じて前記可逆カウンタのカウント数を可変する制御回路を備え、位相調整時間の短縮を図ったことを特徴とする乱数発生装置。

【請求項 4】 電源投入時から一定期間、前記繰り返し周期を通常動作時の繰り返し周期より短くする初期制御回路を備えることを特徴とする請求項 1 から請求項 3 までの何れかに記載の乱数発生装置。

【請求項 5】 前記フリップ・フロップの双方の入力ラインにノイズ発生源とノイズ／位相変換器を付加したことを特徴とする請求項 1 から請求項 4 までの何れかに記載の乱数発生装置。

【請求項 6】 前記フリップ・フロップの何れか片方の入力ラインにノイズ発生源とノイズ／位相変換器を付加したことを特徴とする請求項 1 から請求項 4 までの何れかに記載の乱数発生装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、フリップ・フロップに入力する二つの入力信号の位相差を自動調整してフリップ・フロップ出力の 0 または 1 の出現率が一定になるようにした乱数発生装置に関し、特に効率的な位相調整手段に関するものである。

【0002】

【従来の技術】

高度な科学技術計算やゲーム機、或いは暗号処理等には乱数の使用が不可欠であり、近年、一様性を有し、乱数出現の規則性、前後の相関性、周期性を有しない高性能な乱数発生装置の需要が益々増大してきている。

【0003】

そして、このような乱数発生装置として、フリップ・フロップに入力する二つの入力信号の位相差を自動調整してフリップ・フロップ出力の 0 または 1 の出現率が一定になるようにした乱数発生装置が好適である。係る乱数発生装置は、全てデジタル回路で構成できるため L S I 化への対応が容易で、生産性、コスト性に優れることから、今後の市場規模は極めて膨大である。

【0004】

【発明が解決しようとする課題】

ところで、前記乱数発生装置にあっては、通常、フリップ・フロップ出力（乱

数)の0または1の出現数を監視して、その出現率が、例えば、50パーセントに収束するよう、二つ入力信号の位相差を遅延回路にて自動調整する、いわゆる、フィードバック制御による位相調整手段が採用されるが、特に前記用途に対しては高速性や高性能(高精度)を要求されることから、前記フィードバック制御の応答性が重要な課題であり、所定の出現率に効率良く、且つ高精度で収束できる位相調整手段の実現が望まれている。

【0005】

本発明は、前記要望を満足できる高速で高性能な乱数発生装置を提供することを目的としている。

【0006】

【課題を解決するための手段】

二つの入力部に入力される信号の位相差に応じて出力の状態(0または1)が確定するフリップ・フロップとして、例えば、Dタイプフリップ・フロップが公知である。

このDタイプフリップ・フロップは、図8に示すように、入力部となるクロック端子CLKとデータ端子Dを有し、CLK入力信号の立ち上がり時のデータ端子Dの状態によって出力(Qと/Q)の状態が確定する、所謂エッジトリガ型のフリップ・フロップである。

【0007】

ここで、図9(a)、若しくは図9(b)の状態からCLK信号の立ち上がり時間とD信号の立ち上がり時間の差(位相差) Δt を0に近づけていくと、図9(c)に示すように、フリップ・フロップ出力 Q_n 、 $/Q_n$ が不確定となる位相差の範囲が存在する。そして、このフリップ・フロップの不確定動作範囲は入力信号のジッタが大きくなる程広くなり、乱数の生成を容易にする。

本発明は、このようなフリップ・フロップの不確定動作を積極的に利用した乱数発生装置である。

【0008】

すなわち、請求項1に記載の本発明は、二つの入力信号の位相差に応じて出力の状態(0または1)が確定するフリップ・フロップと、前記入力信号の位相を

調整する位相調整部と、前記入力信号によるフリップ・フロップ出力の 0 または 1 の出現率が所定の繰り返し周期内で一定値に収束するように前記位相差を制御するフィードバック回路部とで構成される乱数発生装置であって、前記位相調整部は、それぞれ順を追って作動する位相の粗調整手段および微調整手段を備えて構成される。

【0009】

また、請求項 2 に記載の本発明は、請求項 1 に記載の乱数発生装置において、前記粗調整手段および微調整手段は、前記入力信号を数段階に遅延し出力する遅延回路と、セレクト入力に応じて遅延出力の何れかを選択する選択回路と、前記位相差に応じて前記セレクト入力を制御する可逆カウンタとで、それぞれ構成される。

前記請求項 1 または請求項 2 に記載の構成では、位相の粗調整、微調整を行うことにより位相調整範囲の拡大と効率的な位相調整が可能となる。

【0010】

また、請求項 3 に記載の本発明は、二つの入力信号の位相差に応じて出力の状態（0 または 1）が確定するフリップ・フロップと、前記入力信号の位相を調整する位相調整部と、前記入力信号によるフリップ・フロップ出力の 0 または 1 の出現率が所定の繰り返し周期内で一定値に収束するように前記位相差を制御するフィードバック回路部とで構成される乱数発生装置であって、前記位相調整部は、前記入力信号を数段階に遅延し出力する遅延回路と、セレクト入力に応じて遅延出力の何れかを選択する選択回路と、前記位相差に応じて前記セレクト入力を制御する可逆カウンタとで構成されており、且つ、0 または 1 の出現率の正規分布と前記繰り返し周期内における 0 または 1 の出現回数を対比し、当該出現回数に対応する前記正規分布の位置に応じて前記可逆カウンタのカウント数を可変する制御回路を備えて構成される。

本構成では、0 または 1 の出現回数が少ない領域では、遅延出力の切換幅を多くして位相の粗調整を行い、正規分布のセンターに近づくに連れて遅延出力の切換幅を小さくして位相を微調整する。これにより、効率的な位相調整が可能となる。

【0011】

また、請求項4に記載の本発明は、請求項1から請求項3までの何れかに記載の乱数発生装置において、電源投入時から一定期間、前記繰り返し周期を通常動作時の繰り返し周期より短くする初期制御回路を備えて構成される。

これにより、電源投入から適切な乱数が生成される迄の期間を短縮できる。

【0012】

また、請求項5に記載の本発明は、請求項1から請求項4までの何れかに記載の乱数発生装置において、前記フリップ・フロップの双方の入力ラインにノイズ発生源とノイズ／位相変換器を付加して構成される。

【0013】

さらに、請求項6に記載の本発明は、請求項1から請求項4までの何れかに記載の乱数発生装置において、前記フリップ・フロップの何れか片方の入力ラインにノイズ発生源とノイズ／位相変換器を付加して構成される。

請求項5または請求項6に記載の構成では、フリップ・フロップに入力される信号にジッタが発生し、フリップ・フロップの不確定動作範囲が広がる。これにより、一様性を有し、規則性や相関性や周期性を有しないより完全な自然乱数を高速、且つ高精度に生成することができるようになる。

【0014】**【発明の実施の形態】**

以下、図面に基づいて本発明に係る乱数発生装置の実施形態を説明する。

【0015】

図1に示すように、本発明の第1実施形態に係る乱数発生装置10は、フリップ・フロップ1と、位相調整部2と、フィードバック回路部3を基本的構成要素としている。

【0016】

ここで、前記フリップ・フロップ1としては、二つの入力部に入力される入力信号（CLOCK）の位相差によって出力の状態（“0”または“1”）が確定する機能を有するフリップ・フロップが使用可能であり、本実施形態では、信号入力用にクロック端子CLKとデータ端子Dを備えた図8に示すDタイプフリッ

プ・フロップを使用している。

【0017】

また、前記位相調整部 2 は、直列に接続され、段階的に遅延量が増加する複数の遅延出力を発生する 2 つの遅延回路 17, 18 (第 1 デイレー 17、第 2 デイレー 18) とセレクト入力に応じてこの遅延出力の何れか一つを選択する選択回路 19 (セレクター 19) と、このセレクト入力を制御する可逆カウンタ 13 (第 3 カウンター 13) で構成され、前記第 1 デイレー 17 と第 2 デイレー 18 の接続点 (遅延中間点となる) が第 1 ノイズ／位相変換器 20 を介して前記フリップ・フロップ 1 のクロック端子 CLK に接続されると共に、セレクター 19 の出力が第 2 ノイズ／位相変換器 21 を介してデータ端子 D に接続されて、フリップ・フロップ 1 に入力される二つの信号の立ち上がり時間の位相差を任意に調整できるように構成されている。

【0018】

また、前記 2 つのノイズ／位相変換器 20, 21 は、前記フリップ・フロップ入りにジッタを生じさせるために、活性状態にある回路素子 (例えば、トランジスタ、抵抗、コンデンサ等) で発生する微弱な熱雑音を利用したノイズ発生源 22, 23 からのノイズを遅延出力に合成する回路である。これにより、フリップ・フロップ 1 の不確定動作範囲が広がり、一様性を有し、且つ、規則性や相関性や周期性を有しないより完全な自然乱数を容易に生成することができるようになる。

尚、このノイズ／位相変換器は、必ずしも、フリップ・フロップ 1 の D 端子と CLK 端子の双方に付加されるものではなく、図 2 に示す乱数発生装置 10 のように、フリップ・フロップ 1 の何れか片方の入力ライン (図 2 では D 端子のみ) に付加するようにしても良く、同様の効果が得られるものである。

【0019】

また、前記フィードバック回路部 3 は、第 1 カウンター 11、第 2 カウンター 12、レジスター 14、比較器 15、定数設定器 16 で構成される。

【0020】

第 1 カウンター 11 は、入力信号 CLOCK から予め決められた繰返し周期 [

CLOCK数 ($2 \times m$)] を計測し、第2カウンタ12は、この繰り返し周期毎に前記フリップ・フロップ出力の“1”（または“0”）の出現数を計測する。また、レジスタ14は第2カウンタ12のカウント値を繰り返し周期毎に取り込んで保持する。尚、カウント値がレジスタ14にセットされる毎に第2カウンタ12は0にクリアされる。定数設定器16はフリップ・フロップ出力の“1”（または“0”）の出現率を設定するための比較データを出力する。本実施形態では、前記繰り返し周期 [CLOCK数 ($2 \times m$)] の $1/2$ の値 (m) が出力されるように予め設定されている。また、比較器15はレジスタ14の保持データ (n) と定数設定器16からの比較データ (m) を比較し、比較結果 ($n > m$) または ($n = m$) または ($n < m$) に対応した比較出力を発生する。第3カウンタ13は、前記比較器15からの比較出力により設定される動作モードにて動作し、そのカウントデータをセレクタ19のセレクト信号として出力する。そして、既述のようにセレクタ19はセレクト信号により選択されたCLOCK信号の所定の遅延信号を出力する。

【0021】

すなわち、上記構成によれば、レジスタ14の出力データ (n) と、この定数設定器16からの出力データ (m) の比較出力に応じて第3カウンタ13が繰り返し周期毎にアップ／ダウン動作（例えば、 $n > m$ 時はカウントアップ (+1)、 $n < m$ 時はカウントダウン (-1)）を行い、比較器15の比較出力が $n = m$ ($n = m$ 時はカウント動作を停止 (± 0) し、CLOCK信号の位相差は一定を維持する) に収束するようにフリップ・フロップ1のデータ端子Dに入力されるCLOCK信号の立ち上がり時間を自動的に補正する。具体的には、図9 (c) のように、CLK信号の立ち上がりとD信号の立ち上がりの位相差 Δt が0に近づいていくように制御される。これにより、フリップ・フロップ1の出力に“0”と“1”の出現率が常時50%に維持された一様性のある1bitのシリアル乱数データOUTが得られる。

【0022】

以上が乱数発生装置10の基本動作であるが、本実施形態では、前記第1カウンタ11に初期制御回路24を接続し、電源投入時から一定クロック数だけ、

第1カウンタ11の通常動作時のカウンタ設定値 ($2 \times m$) を強制的に $m = 1$ とするようにしている。これにより、電源投入時に確率を $1/2$ に効率良く収束することができ、位相調整期間の短縮化が図れるようになる。

【0023】

次に図3に基づいて本発明の第2実施形態を説明する。

本実施形態の乱数発生装置10の基本構成は、図1と同様、フリップ・フロップ1と、位相調整部2と、フィードバック回路部3より構成されるが、図1とは位相調整部2の構成が相違している。

【0024】

即ち、本構成は、第3カウンタ13、第1セレクタ19、第1ディレー17、第2ディレー18で成る位相調整回路を微調整手段として用い、各々の遅延出力に第3ディレー31、第2セレクタ32で成る粗調整手段と第4ディレー33、第3セレクタ34で成る粗調整手段を付加し、前記第2セレクタ32および第3セレクタ34のセレクト動作を第4カウンタ30の出力にて指定するものである。因みに、微調整用の第1ディレー17と第2ディレー18の1ステップ当たりの遅延時間は粗調整用の第3ディレー31と第4ディレー33の遅延時間に比べて約 $1/20$ 以下に設定されている。また、この第4カウンタ30は比較器15の比較出力にて制御されるもので、そのカウンタ動作は第3カウンタ13の場合と同様である。

【0025】

以下、図4および表1を参照して図3に示した乱数発生装置10による位相の粗調整動作および微調整動作を説明する。尚、図4は位相調整時の粗調整と微調整の動作範囲を示し、表1はその際の第3カウンタ13と第4カウンタ30の動作テーブルを示している。ここで、微調整範囲は $[0 \sim r \times (g - 1)]$ 、粗調整範囲は $[-s \times (h) \sim s \times (h - 1)]$ とする。

初期状態において、粗調整用の第4カウンタ30のカウント値 (SN) と微調整用の第3カウンタ13のカウント値 (RN) は共に0とする。初期制御回路24により電源投入時に第1カウンタ11の (m) を一定クロック数 (図4における位相調整幅 t_{dw} 、即ち、 $2 \times (2 \times g + h)$ クロック数) だけ強制的

に $m=1$ に制御されるため、この一定期間、第3カウンタ13は比較器15の比較出力に基づいて2クロック毎にカウント動作（+1、または±0、または-1）することになる。また、この間、第4カウンタ30は、比較器15の比較出力と前記第3カウンタ13の状態に基づいてカウント動作（+1、または±0、または-1）する。

【0026】

先ず、（1）最終的に調整される位相ポイントが図4中のa1にある場合は、電源投入時、第3カウンタ13は比較器15の比較出力（ $n < m$ ）により2クロック毎に0から（ $g-1$ ）までカウントアップする。

第3カウンタ13が $RN = (g-1)$ にカウントアップすると、次ぎの2クロックで第4カウンタ30が2クロック毎に比較器15の比較出力（ $n < m$ ）と前記第3カウンタ13の $RN = (g-1)$ の状態を条件として0から（ $h-2$ ）までカウントアップし、 $SN = (h-2)$ となる。ここで、 $SN = (h-2)$ の状態は、図4中で位相設定ポイントa1に対応する粗調整ステップ位置であり、これに対応する微調範囲は、図4中の（イ）の範囲 $[0 \sim r \times (g-1)]$ となる。係るカウンタ動作中、第3カウンタ13の $RN = (g-1)$ の状態は初期制御回路24の制御の基で強制的に保持されている。

次に、第3カウンタ13が $RN = (g-1)$ 、第4カウンタ30が $SN = (h-2)$ の状態、比較器15の比較出力（ $n > m$ ）により第3カウンタ13が2クロック毎にカウントダウンして位相設定ポイントa1に逐次近付いて行き、フリップ・フロップ出力の“1”の出現率が $1/2$ に収束されるように自動的に位相が調整され、最終的に前記位相設定ポイントa1の位相前後に留まることになる。

【0027】

また、（2）最終的に調整される位相がa2の場合は、初期状態において、 $SN = (0)$ 、 $RN = (0)$ である。第3カウンタ13が $RN = (0)$ であると、比較器15の比較出力（ $n > m$ ）により、次ぎの2クロックで第4カウンタ30が2クロック毎に（0）から（-2）にカウントダウンし、 $SN = (-2)$ となる。ここで、 $SN = (-2)$ の状態は、図4中で位相設定ポイントa2に対

応する粗調整ステップ位置 ($-s \times 2$) であり、微調整範囲は、図 4 中の (ロ) の範囲 $[0 \sim r \times (g-1)]$ となる。係るカウンタ動作中、第 3 カウンタ 13 の $RN = (0)$ の状態は初期制御回路 24 の制御の基で強制的に保持されている。

次に、第 3 カウンタ 13 が $RN = (0)$ 、第 4 カウンタ 30 が $SN = (-2)$ の状態から、比較器 15 の比較出力 ($n < m$) により第 3 カウンタ 13 が 2 クロック毎にカウントアップして位相設定ポイント a2 に逐次近付いて行き、最終的にフリップ・フロップ出力の“1”の出現率が $1/2$ に収束されるように自動的に調整され、前記位相設定ポイント a2 の位相前後に留まることになる。

【0028】

次に、(3) 初期制御動作により位相設定ポイントが a1 または a2 に調整された以降の通常動作では、表 1 に示すように、第 3 カウンタ 13 は、 $RN = (0)$ または $RN = (g-1)$ 以外の時、第 1 カウンタ 11 で設定した m (例えば $m = 250$) による一定期間 ($2 \times m$ のクロック毎) に比較器 15 の比較出力に基づくカウント動作 ($+1$ 、 ± 0 、 -1) が行われる。

また、 $RN = (0)$ の時、第 3 カウンタ 13 は、比較器 15 の比較出力に基づいて $[+1$ 、 ± 0 、 $RN(g-1)]$ のカウント動作を行い、第 4 カウンタ 30 は第 3 カウンタ 13 が $RN(g-1)$ に移行する時 -1 される。

また、 $RN = (g-1)$ の時、第 3 カウンタ 13 は、比較器 15 の比較出力に基づいて $[+1$ 、 ± 0 、 $RN(g-1)]$ のカウント動作を行い、第 4 カウンタ 30 は第 3 カウンタ 13 が $RN = (0)$ に移行する時 $+1$ される。

【0029】

以上のように、先ず始めに、所定の位相まで大まかに位相が調整され(粗調整)、その後、最終的に調整される位相設定ポイントに微調整されて行く。これにより、高精度の位相調整が効率的に行われ、フィードバック制御による位相調整の高速化が可能となる。また、粗調整手段を設けることで、少ない遅延ステップ構成で広い位相調整幅が得られるようになり、位相調整部 2 を構成する回路部品を削減できる。

【0030】

【表 1】

第 3 カウンター	比較器	初期動作時 ($m = 1$)		通常動作時 (m は任意)	
		第 3 カウンター	第 4 カウンター	第 3 カウンター	第 4 カウンター
RN = (0)	$n > m$	± 0	-1	$RN = (g-1)$	-1
	$n = m$	± 0	± 0	± 0	± 0
	$n < m$	$+1$	± 0	$+1$	± 0
$0 < RN < (g-1)$	$n > m$	-1	± 0	-1	± 0
	$n = m$	± 0	± 0	± 0	± 0
	$n < m$	$+1$	± 0	$+1$	± 0
RN = (g-1)	$n > m$	-1	± 0	-1	± 0
	$n = m$	± 0	± 0	± 0	± 0
	$n < m$	± 0	$+1$	RN = (0)	$+1$

【0031】

次に、図5～図7に基づいて本発明の第3実施形態を説明する。

ここで、図6は一様性を有した乱数発生装置により乱数を1,000回出力した時の“1”または“0”の出現回数をプロットした図で、正規分布を示す。図7はこの正規分布をセンター基準に等間隔で8分割し、センターを ± 0 として総計10個の各分割位置に対して図7中、右端から $+5 \sim -5$ の重み付けをしたものである。

【0032】

図5に示す乱数発生装置10は、図1の乱数発生装置10における比較器15の比較形態をマルチに変えると共に、その出力に制御回路40を接続して構成したものである。本実施形態では、レジスター14の内容(n)と比較する比較器15の比較データを、図7に示す正規分布のマルチ分割位置データ($m + 4 \times k$) \sim ($m - 4 \times k$)としており、前記出現回数のカウント数が正規分布のどの分割位置に対応するかを即座に出力できるように構成されている。

【0033】

また、前記制御回路40は、比較器15の比較出力($(n > m + 4 \times k) \sim$

$n > m - 4 \times k$)) より分割位置データに対応する重み付け ($-5 \sim +5$) を判断し、それにそれに応じたカウント数を第3カウンタ13にセットする。第3カウンタ13は重み付けに応じたカウント動作を行い、セレクタ19による遅延出力の切換幅 (切換ステップ数) を制御する。例えば、重み付けが (-4) であれば、第3カウンタ13は一回の動作でダウンカウントを4回繰り返し、重み付けが ($+3$) であれば、1回の動作でアップカウントを3回繰り返す。また、重み付けが (0) であれば、カウント動作は停止している。

【0034】

このように、本構成では、“0” または “1” の出現回数が少ない正規分布領域 (例えば、図7において出現回数が450或いは550の近傍) では、重み付けにより遅延出力の切換幅を多くして位相の粗調整を行い、正規分布のセンターに近づくに連れて (図7における出現回数が500の近傍) 遅延出力の切換幅を小さくして位相を微調整する。これにより、効率的な位相調整が可能となる。

【0035】

以上説明した第1～第3実施形態では、乱数発生用のフリップ・フロップとしてDタイプフリップ・フロップを用いたが、本発明はこれに限定されるものではなく、これと同等の機能を有するフリップ・フロップであれば使用可能であり、例えば、R-Sフリップ・フロップ等が使用できる。

【0036】

また、本発明のシリアル型乱数発生装置10をP個並列に配置することにより、Pビット構成の並列型乱数発生装置を構成することもできる。

【0037】

さらに、上記したシリアル型乱数発生装置や並列型乱数発生装置を用いれば、一様性を有し、規則性、相関性、周期性を有さない高速・高性能の確率発生装置を実現することもできる。

【0038】

【発明の効果】

以上説明したように、本発明によれば、フィードバック制御による位相調整において、位相調整部に粗調整手段と微調整手段を設けたので、効率的な位相調整

が可能となり、乱数発生的高速化が図れる。また、粗調整手段を設けることで、少ない遅延ステップ構成で広い位相調整幅が得られるようになり、その分、回路部品も削減できる。

【0039】

また、本発明によれば、乱数の0または1の出現率の正規分布と実際の出現回数を対比し、当該出現回数に対応する正規分布の位置に応じて位相調整幅を可変するようにしたので、上記同様に効率的な位相調整が可能となり、乱数発生的高速化が図れる。

【図面の簡単な説明】

【図1】

本発明の第1実施形態に係る乱数発生装置の構成を示す図。

【図2】

本発明の第1実施形態に係る乱数発生装置の図1とは別の構成を示す図。

【図3】

本発明の第2実施形態に係る乱数発生装置の構成を示す図。

【図4】

位相調整時の粗調整と微調整の動作範囲を示す図。

【図5】

本発明の第3実施形態に係る乱数発生装置の構成を示す図。

【図6】

一様性を有する乱数の正規分布を示す図。

【図7】

図6の正規分布を分割し、重み付けした図。

【図8】

Dタイプフリップ・フロップを示す図。

【図9】

図8のDタイプフリップ・フロップの入出力波形を示す図。

【符号の説明】

1 フリップ・フロップ

2 位相調整部

3 フィードバック回路部

1 0 乱数発生装置

1 3, 3 0 可逆カウンタ (カウンター)

1 7, 1 8, 3 1, 3 3 遅延回路 (ディレー)

1 9, 3 2, 3 4 選択回路 (セレクター)

2 0, 2 1 ノイズ／位相変換器

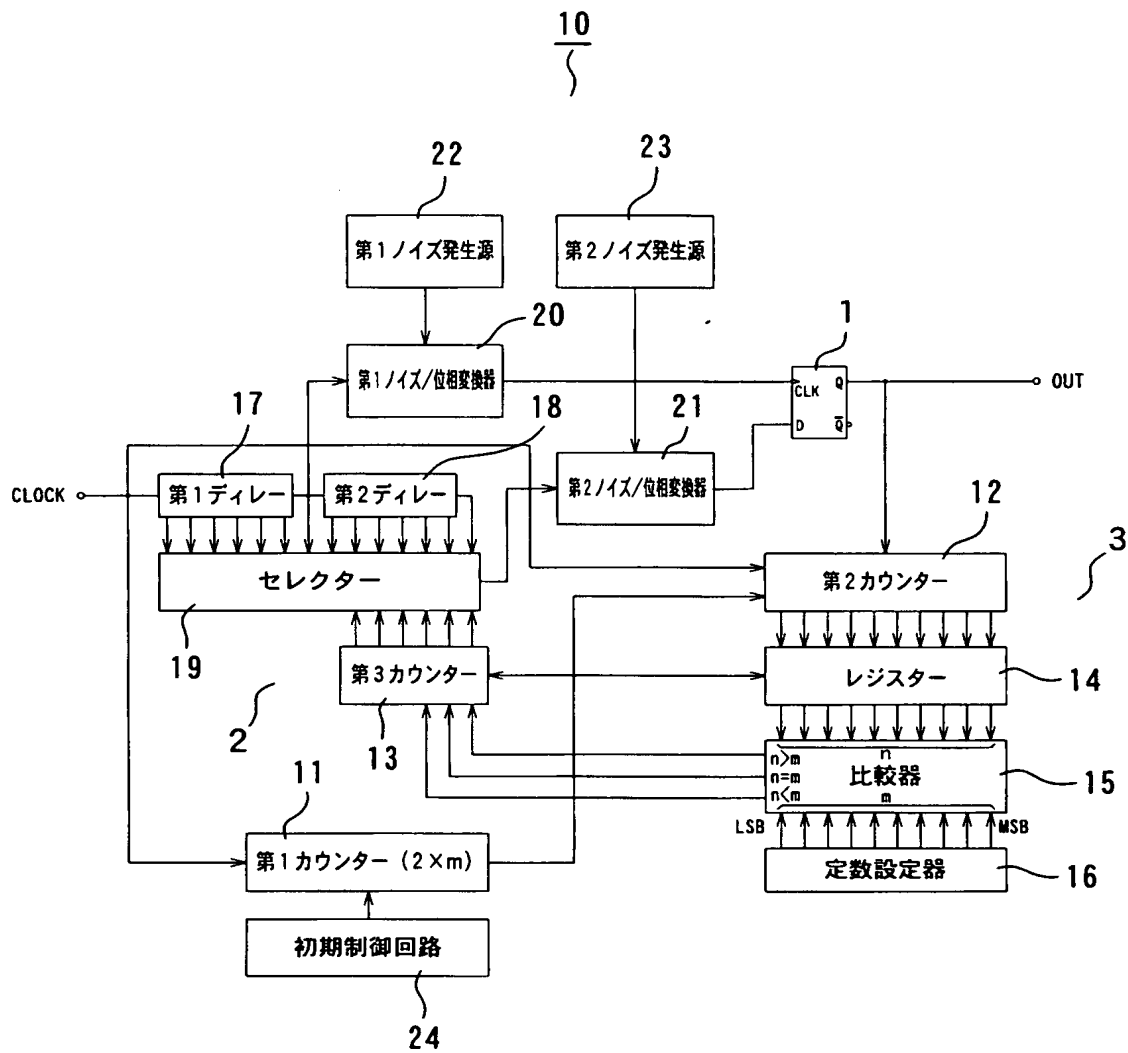
2 2, 2 3 ノイズ発生源

2 4 初期制御回路

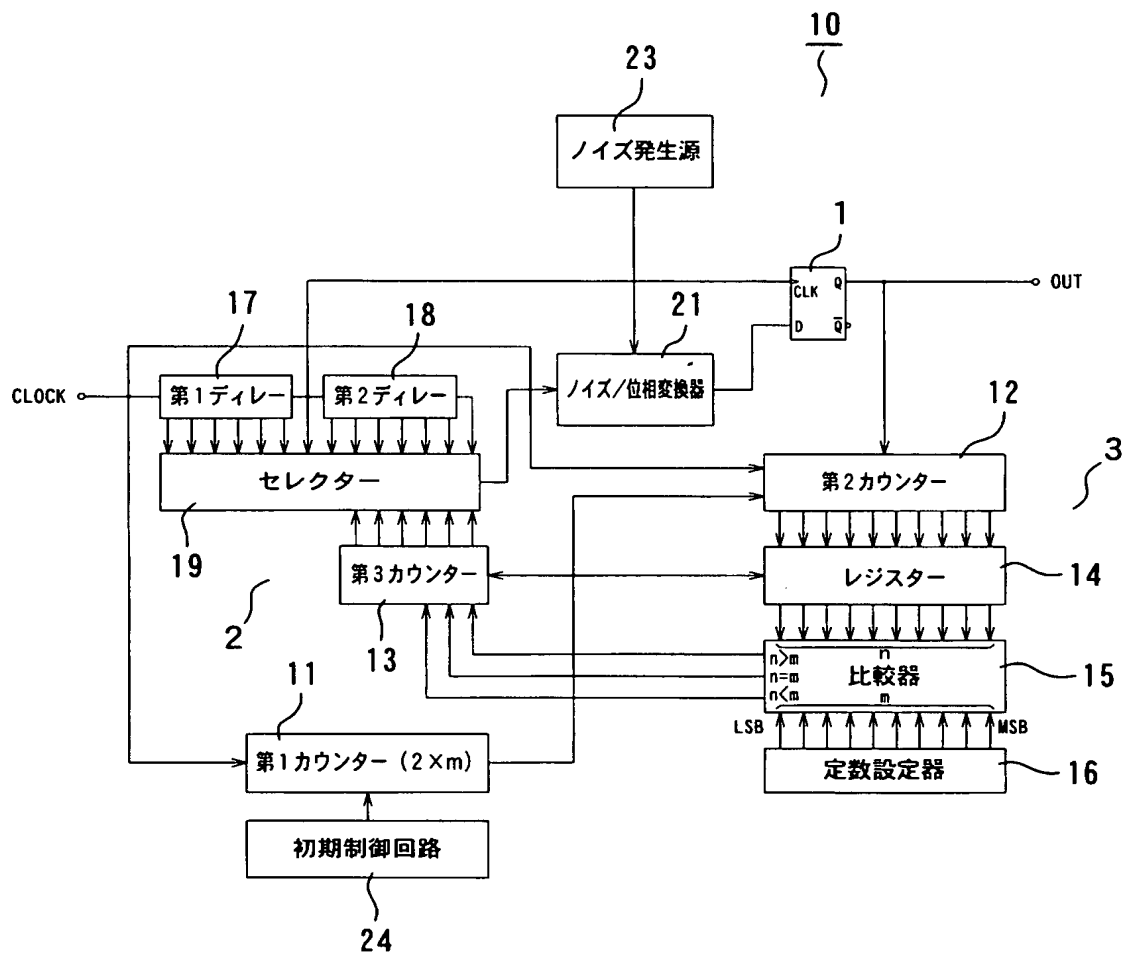
1 制御回路

【書類名】 図面

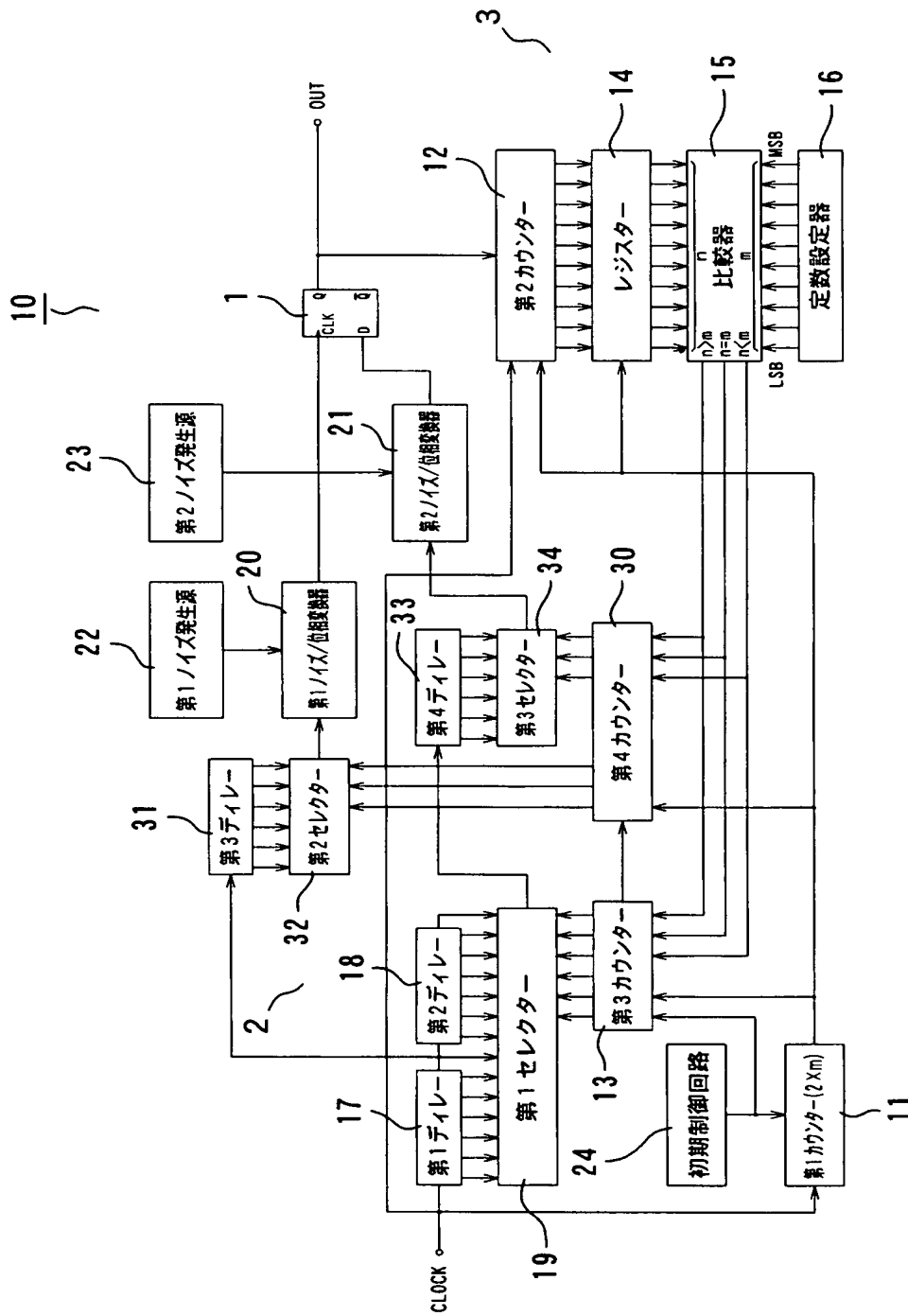
【図 1】



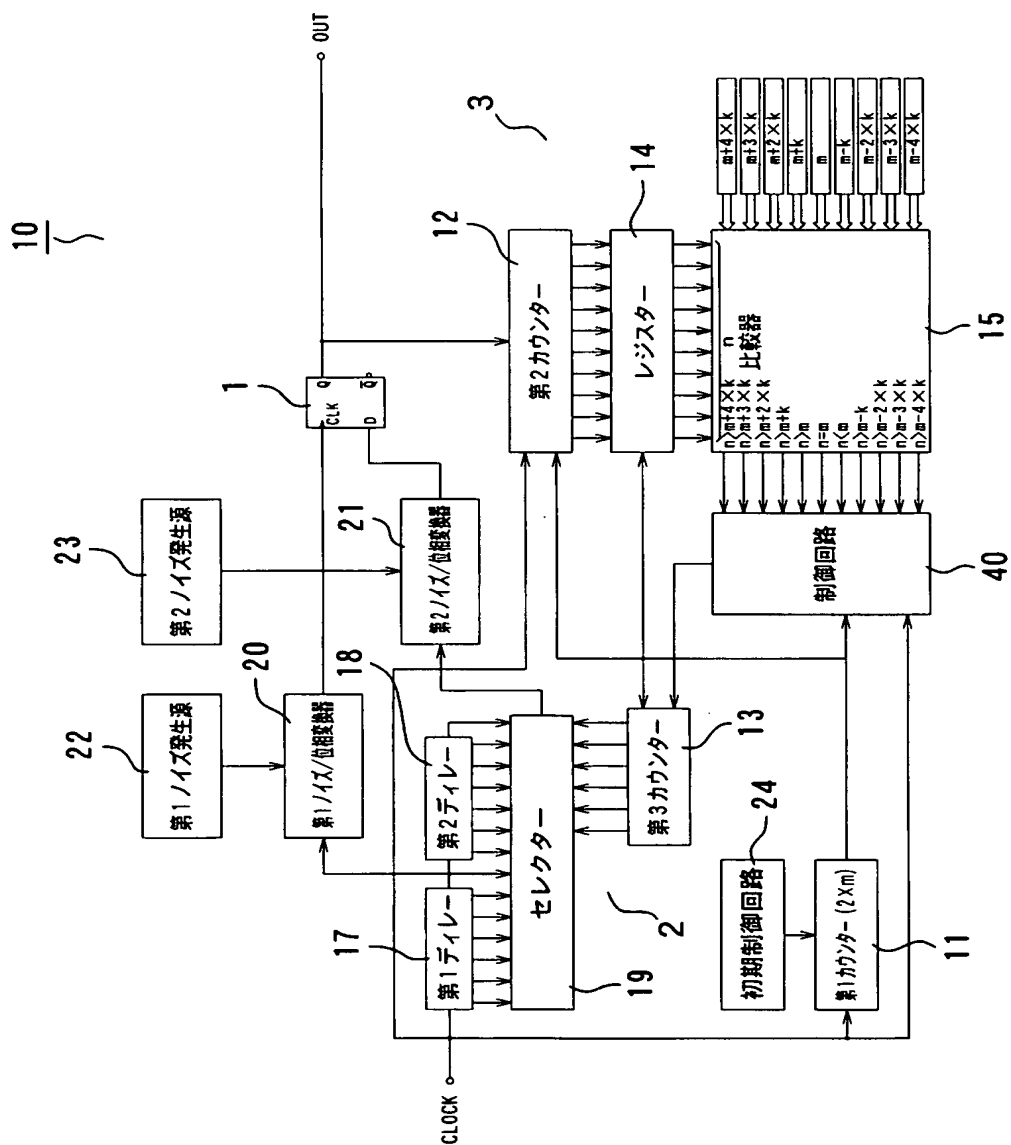
【図 2】



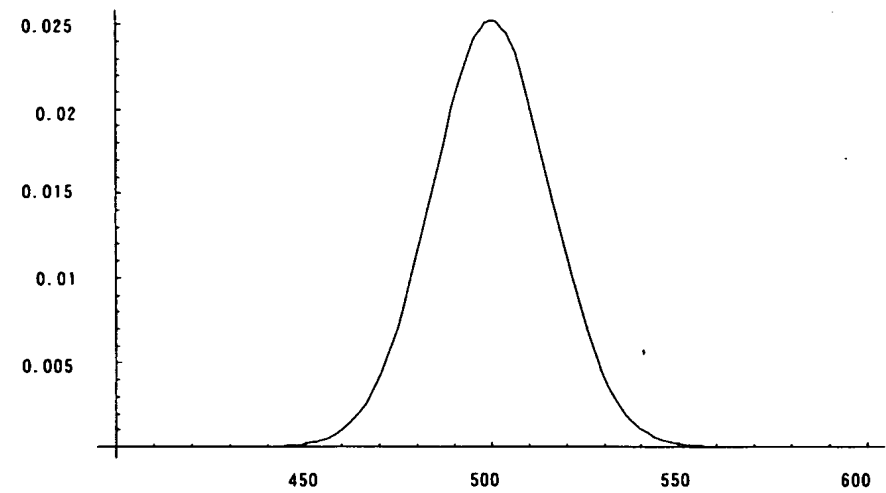
【図3】



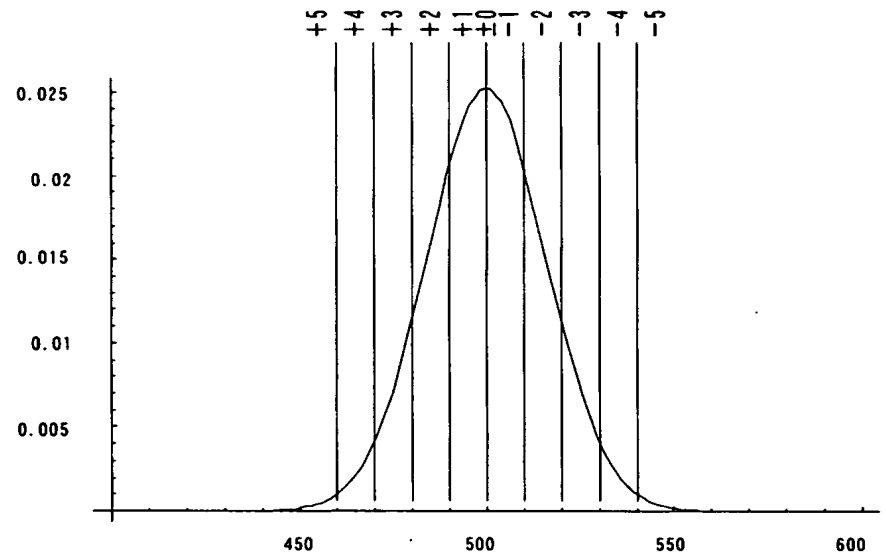
【図 5】



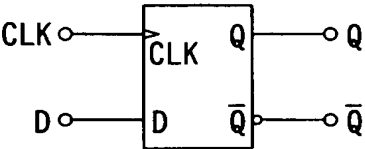
【図 6】



【図 7】

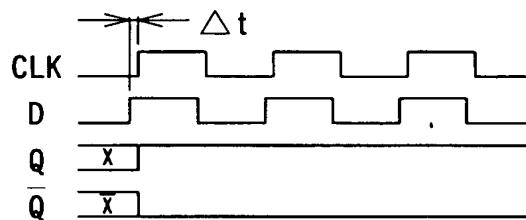


【図 8】

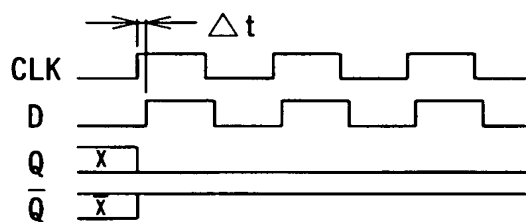


【図 9】

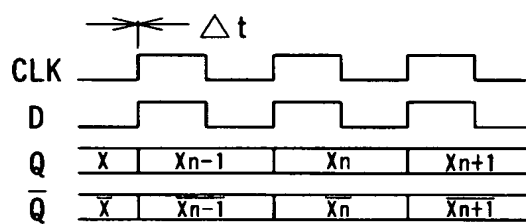
(a)



(b)



(c)



【書類名】 要約書

【要約】

【課題】 一様性を有し、規則性、相関性、周期性を有しない高速・高性能な乱数発生装置を提供する。

【解決手段】 乱数発生装置 1 0 は、二つの入力信号の位相差に応じて出力の状態（0 または 1）が確定するフリップ・フロップ 1 と、前記入力信号の位相を調整する位相調整部 2 と、前記入力信号によるフリップ・フロップ出力の 0 または 1 の出現率が所定の繰り返し周期内で一定値に収束するように前記位相差を制御するフィードバック回路部 3 とで構成される。ここで、前記位相調整部 2 は、それぞれ順を追って作動する位相の粗調整手段および微調整手段を備えている。本構成により、位相調整幅の拡大と位相調整時間の短縮が可能となり、乱数発生的高速化が図れる。

【選択図】 図 3

認定・付加情報

特許出願の番号	特願 2 0 0 1 - 2 1 7 7 1 0
受付番号	5 0 1 0 1 0 5 5 1 7 6
書類名	特許願
担当官	第八担当上席 0 0 9 7
作成日	平成 1 3 年 7 月 1 9 日

＜認定情報・付加情報＞

【提出日】 平成13年 7月18日

次頁無

【書類名】 出願人名義変更届（一般承継）
【整理番号】 IP01401
【あて先】 特許庁長官 殿
【事件の表示】
 【出願番号】 特願2001-217710
【承継人】
 【識別番号】 000237721
 【氏名又は名称】 エフ・ディー・ケイ株式会社
【承継人代理人】
 【識別番号】 100067046
 【弁理士】
 【氏名又は名称】 尾股 行雄
 【電話番号】 03-3543-0036
【提出物件の目録】
 【包括委任状番号】 0014478
 【物件名】 閉鎖事項全部証明書 1
 【援用の表示】 特願 2 0 0 1 - 1 7 0 6 5 2
 【物件名】 履歴事項全部証明書 1
 【援用の表示】 特願 2 0 0 1 - 1 7 0 6 5 2
【プルーフの要否】 要

認定・付加情報

特許出願の番号	特願 2 0 0 1 - 2 1 7 7 1 0
受付番号	5 0 2 0 0 8 8 8 5 9 2
書類名	出願人名義変更届（一般承継）
担当官	金井 邦仁 3 0 7 2
作成日	平成 1 4 年 7 月 1 0 日

< 認定情報・付加情報 >

【提出日】	平成14年 6月19日
-------	-------------

次頁無

特願 2 0 0 1 - 2 1 7 7 1 0

出 願 人 履 歴 情 報

識別番号

[3 9 0 0 2 2 7 9 2]

1 . 変更年月日

1 9 9 0 年 1 1 月 1 3 日

[変更理由]

新規登録

住 所

東京都港区新橋 5 丁目 3 6 番 1 1 号

氏 名

いわき電子株式会社

特願 2 0 0 1 - 2 1 7 7 1 0

出 願 人 履 歴 情 報

識別番号

[0 0 0 2 3 7 7 2 1]

1 . 変更年月日

1 9 9 0 年 8 月 2 9 日

[変更理由]

新規登録

住 所

東京都港区新橋 5 丁目 3 6 番 1 1 号

氏 名

富士電気化学株式会社

2 . 変更年月日

2 0 0 1 年 1 月 1 6 日

[変更理由]

名称変更

住 所

東京都港区新橋 5 丁目 3 6 番 1 1 号

氏 名

エフ・ディー・ケイ株式会社